

Managing Clusters of Switches

A cluster is a group of connected switches that are managed as a single entity. The switches can be in the same location, or they can be distributed across a Layer 2 contiguous network. All communication with cluster switches is through one IP address. You can have up to 16 switches in a cluster: 1 *command* switch and 15 *member* switches. The command switch is the single point of access used to configure and monitor the member switches. A member switch is managed through a command switch.

Command switches must be running IOS Release 12.0(5)XP software that supports the ability to be a command switch. For the complete list of command-capable switches, see the “Supported Hardware” section on page 1-3. This section also describes the required software for member switches.

This chapter describes how to create and manage clusters of switches by using the three components of the Cluster Management software: Cluster Builder, Cluster Manager, and Cluster View. You use Cluster Builder to build the cluster and perform some minor configuration tasks. You use Cluster Manager to monitor, manage, and configure switches in the cluster. You use Cluster View to display the cluster as a double-switch icon and see connections to devices outside of the cluster.

For information about the Cluster Management interface and navigation techniques, see Chapter 2, “Using the Management Interfaces.”

This chapter describes how to perform the following tasks:

- Plan your cluster
- Create clusters
- Manage clusters
- Display link utilization graphs

- Display device reports and graphs
- Perform individual device configuration

Planning Your Cluster

How you create a cluster depends on your network. If the switches are arrayed in a star topology with the command switch at the center, you can add all the *candidate switches* to the cluster at once. Candidate switches are fully qualified to become member switches.

If the switches are connected in a daisy-chain topology, you add the candidate connected to the command switch and then continue adding each switch in the chain as it is discovered by CDP. If switches are daisy-chained off of a star topology, you can add all the switches directly connected to the command switch and then add the daisy-chained switches one at a time.

In addition, you must configure the cluster switches and candidates to be in the same management VLAN if you want to manage them in a cluster.

Command Switch Requirements

You must select a switch to be the command switch of your cluster. The command switch must satisfy the following requirements:

- It is running command-capable clustering software (see “Supported Hardware” section on page 1-3) with the command switch functionality enabled.
- It is assigned an IP address (optional if you perform the configuration with the CLI).
- It has CDP version 2 enabled.
- It is not a command or member switch of another cluster.
- It must belong to the same management VLAN as its member switches.

Candidate Switch Requirements

Before adding a candidate switch to the cluster, you must know its enable or enable secret password if one has been assigned.

A candidate switch must satisfy the following requirements to join a cluster:

- It is running cluster-capable software (see “Supported Hardware” section on page 1-3).
- It has CDP version 2 enabled.
- It is connected to a command switch through ports that belong to the same management VLAN (see “Changing the Management VLAN on Candidate Switches” section on page 4-5).
- It is not an active member or command switch of another cluster.

A candidate switch can have an IP address, but it is not required.

Note Be aware that after adding a candidate to the cluster, some configurations can prevent the command switch from maintaining contact with member switches. If you are unable to maintain management contact with a member, see the “Recovering from Lost Member Connectivity” section on page 5-12.

Replacement Command Switch Requirements

If the command switch fails, member switches continue forwarding data traffic but cannot be managed through the command switch. Member switches retain the ability to be managed through normal standalone means, such as the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after you assign an IP address to them.

You can recover from a failed command switch by replacing the failed switch with a cluster member or another switch that is command capable. For the list of switches that can be command switches, see “Supported Hardware” section on page 1-3.

To replace the command switch, you must assign an IP address to the replacement switch, if it does not already have one, and know the command switch password. If you are using Telnet to manage the switch, you also need to know the login password. For the actual recovery procedures, see the “Recovering from a Command Switch Failure” section on page 5-7.

Changing the Management VLAN on an Existing Cluster

To manage switches in a cluster, the port connections among the command, member, and candidate switches must all be on the same VLAN as the management VLAN. You only need to change the management VLAN on your cluster switches if you have an upstream device, such as a Catalyst 5000 switch, configured in a different management VLAN. Otherwise, Cisco recommends that you leave the management VLAN set to VLAN 1, the default setting.

Note To avoid loss of connectivity to your switches, perform the procedure in the specified order. Cisco recommends that you perform this reconfiguration only with the CLI through a console connection.

To change the management VLAN on an existing cluster, review the section “Guidelines for Changing the Management VLAN” section on page 3-55 and then follow these steps:

Step 1 Change the management VLAN on each member (do not include the command switch).

For instructions, see the “CLI Procedure for Configuring the Management VLAN Interface through a Console Connection” section on page 3-55.

Note Do not try this procedure using the **rcommand** command or a Telnet connection.

Step 2 Make sure connectivity exists among the member switches and the command switch on the new management VLAN.

For example, reassign the member and command switch static-access ports or multi-VLAN ports to be in the same VLAN as the new management VLAN. See the “CLI Procedure for Assigning Static-Access Ports to a VLAN” section on page 3-103 and “CLI Procedure for Assigning Ports for Multi-VLAN Membership” section on page 3-104.

Step 3 Change the management VLAN on the command switch.

For instructions, see the “CLI Procedure for Configuring the Management VLAN Interface through a Console Connection” section on page 3-55.

Changing the Management VLAN on Candidate Switches

Before adding a candidate switch whose management VLAN is other than VLAN 1, review the section “Guidelines for Changing the Management VLAN” section on page 3-55 and then follow these steps:

Note To avoid loss of connectivity to your switches, perform the procedure in the specified order. Cisco recommends that you perform this reconfiguration only with the CLI through a console connection.

Step 1 Make sure there is connectivity to the command switch on the cluster management VLAN.

For example, configure the member and command switch static-access ports or multi-VLAN ports to be in the same VLAN as the cluster. See the “CLI Procedure for Assigning Static-Access Ports to a VLAN” section on page 3-103 and “CLI Procedure for Assigning Ports for Multi-VLAN Membership” section on page 3-104.

Step 2 Configure the management VLAN on the candidate switch to be the same as that of the cluster.

For instructions, see the “CLI Procedure for Configuring the Management VLAN Interface through a Console Connection” section on page 3-55.

Creating Clusters

After you assign an IP address to the command switch, enable the command functionality, and connect it to other switches running clustering software, you can use Cluster Builder to create a cluster managed through one IP address. The command switch begins an automatic discovery of candidate switches and uses information from Cisco Discovery Protocol (CDP) to identify candidate switches.

After the cluster is formed, you can access all switches in the cluster by entering the IP address of the command switch into the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer). The password you enter when you log into the command switch gives you access to member switches. If the command switch fails, you can use its password to create a new command switch for the cluster. For more information, see “Recovering from a Command Switch Failure” section on page 5-7.

Enabling the Command Switch

You enable the command switch functionality on the CVSM home page or through the CLI. If a switch is not command capable, you will not be able to enable the function or name the cluster. You can use up to 31 characters to name your cluster.

After you have enabled the command switch and named the cluster in CVSM, click **Cluster Management** to begin building your cluster through Cluster Builder.

You can also build your cluster through the CLI. For more information, see the “CLI Procedure for Creating the Cluster” section on page 4-11.

Automatically Discovering Cluster Candidates

The command switch discovers neighbors directly connected to the cluster. Each time a new member is added to the cluster, the next discovery is extended one hop from the cluster members. When the application starts and when the topology changes, Cluster Builder automatically prompts you to add prequalified candidates. With each new discovery, it displays the Suggested Candidate window (Figure 4-1) so that you can add switches to the cluster. The Suggested Candidate window lists the discovered candidate switches with their device types, MAC addresses, and the upstream switch through which it is directly connected to the cluster.

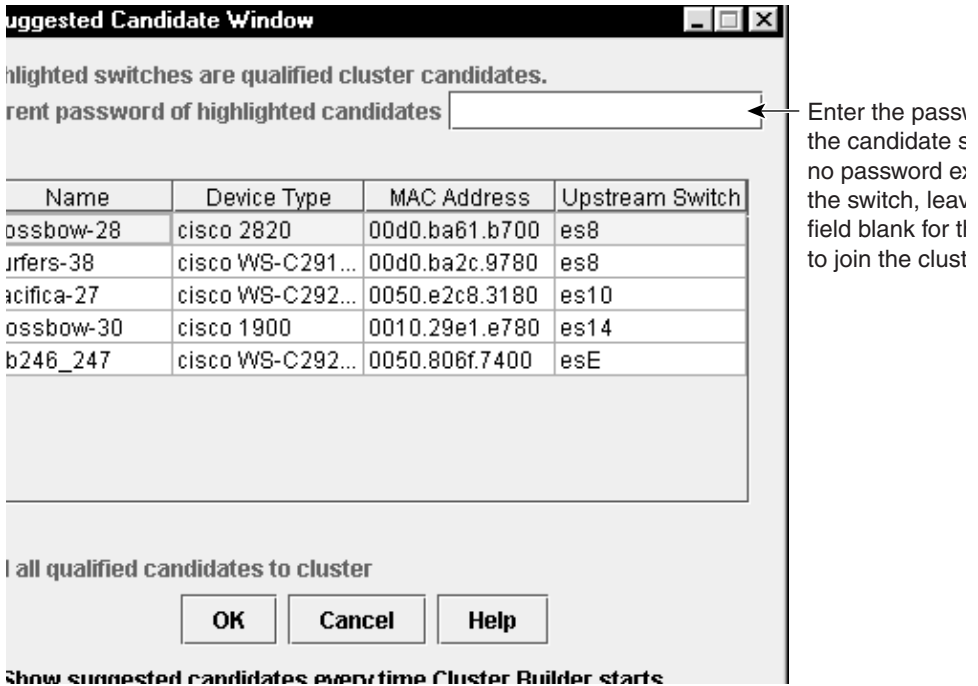
By default, the suggested candidates are highlighted in the window, but you can select one or multiple switches as long as the number of switches selected does not exceed the maximum number for the cluster. You can accept the suggested candidates or not. If you do not accept the suggested candidates, none of the switches are added, and you must add them one at a time. If you accept the suggested candidates and there are more switches daisy-chained to a cluster member, you must add them one at a time.

When you accept the suggested candidates, enter the password if one has been defined. If no password has been defined, click **OK** to add it to the cluster with no password. If you enter a password that does not match the password defined for the candidate, or if you enter a password for a candidate that does not have a password defined for it, the candidate is not added to the cluster. In all cases, once a candidate switch joins a cluster, it inherits the command switch password. For more information on setting passwords, see the “Changes to Passwords” section on page 4-10.

Note The Suggested Candidates window displays prequalified candidates whether or not they are in the same management VLAN as the command switch. If you enter the password for a candidate in a different VLAN than the cluster and click **OK**, this switch is not added to the cluster. It appears as a candidate switch in Cluster Builder. For information on how to change the management VLAN, see the “Changing the Management VLAN on Candidate Switches” section on page 4-5.

You can set Cluster Builder to not automatically display suggested candidates. For more information, see the “Changing User Settings” section on page 4-17.

Figure 4-1 Suggested Candidate Window



When the Cluster is Created

When a cluster is formed, the command switch automatically makes configuration changes to the member switch host name, password, and SNMP community string.

Changes to the Host Name

If you did not assign a host name to a member switch, the command switch appends a unique member number to its own host name and assigns it sequentially to the switch when it joins the cluster. The number indicates the order in which the switch was added to the cluster. For example, a command switch named *eng-cluster* could name cluster member 5 *eng-cluster-5*.

If you did not assign a host name to the command switch, it keeps the default host name of *Switch*.

If you assigned a host name to the member switch, it retains that name when it joins the cluster. However, if your switch was part of a cluster, received its host name from the command switch, was removed and then readded to a new cluster, its host name (such as *eng-cluster-5*) is overwritten with the new version of the command switch host name.

Changes to the SNMP Community Strings

The following SNMP community strings are added to a member switch when it joins a cluster:

- `commander-readonly-community-string@esN`, where N is the member switch number.
- `commander-readwrite-community-string@esN`, where N is the member switch number.

If the command switch has multiple read-only or read/write community strings, only the first read-only and read/write strings are propagated to the member switch.

The Catalyst 2900 and 3500 XL switches support an unlimited number of community strings and string lengths.

The Catalyst 1900 and 2820 switches support up to four read-only and four read/write community strings; each string contains up to 32 characters. When these switches join the cluster, the first read-only and read/write community string on the command switch is propagated and overwrites the fourth read-only and read/write community string on the member switches. To support the 32-character string-length limitation on the Catalyst 1900 and 2820 switches, the command switch community strings are truncated to 27 characters when propagating them to these switches, and the `@esN` (where N refers to the member switch number and can be up to two digits) is appended to them.

For more information about configuring community strings through Cluster Manager, see the “Configuring SNMP” section on page 4-31.

Changes to Passwords

The member switch inherits the command switch enable secret or enable password when it joins the cluster and retains it when it leaves the cluster. If no command switch password is configured, the member switch inherits a null password. Member switches also inherit the command switch password privilege level 15.

However, certain caveats apply to Catalyst 1900 and 2820 switches as cluster members. Their passwords and privilege levels are altered in the following ways:

- Password length
 - If the command switch enable password is longer than 8 characters, the member switch enable password is truncated to 8 characters.
 - If the command switch enable password is between 1 and 8 characters inclusive, the member switch enable password will be the same as the command switch password. (Though the password length for Catalyst 1900 and 2820 switches is from 4 to 8 characters, the length is only checked when the password is configured from the menu console or with the CLI.)
 - Both the command switch and member switch support up to 25 characters (52 characters encrypted) in the enable secret password.
- Privilege level

The command switch supports up to 15 privilege levels. Catalyst 1900 and 2820 member switches support only levels 1 and 15.

 - Command switch privilege levels 1 to 14 map to level 1 on the member switch.
 - Command switch privilege level 15 maps to level 15 on the member switch.

CLI Procedure for Creating the Cluster

This procedure assumes that the candidate switch has connectivity to the command switch through the same VLAN and is in the same management VLAN. For more information, see the “CLI Procedure for Assigning Static-Access Ports to a VLAN” section on page 3-103, “CLI Procedure for Assigning Ports for Multi-VLAN Membership” section on page 3-104, and “CLI Procedure for Configuring the Management VLAN Interface through a Console Connection” section on page 3-55.

Beginning in privileged EXEC mode on the command switch, follow these steps to enable the command switch and add candidate switches to the cluster:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enable the command switch and name the cluster (up to 31 characters).	cluster enable <i>name</i>
Step 3 Return to privileged EXEC mode.	end
Step 4 Display a list of candidates.	show cluster candidates
Step 5 Display a list of current cluster members.	show cluster members
Step 6 Enter global configuration mode.	configure terminal
Step 7 Add candidates to the cluster. Assign a unique number from 1 to 15 for <i>n</i> . Do not use any switch number (SN) that appears in the show cluster members display. Enter the candidate switch MAC address, which can be obtained from the show cluster candidates display.	cluster member <i>n</i> mac-address <i>hw-addr</i> password <i>password</i>
Step 8 Return to privileged EXEC mode.	end
Step 9 Display the status of the cluster.	show cluster members

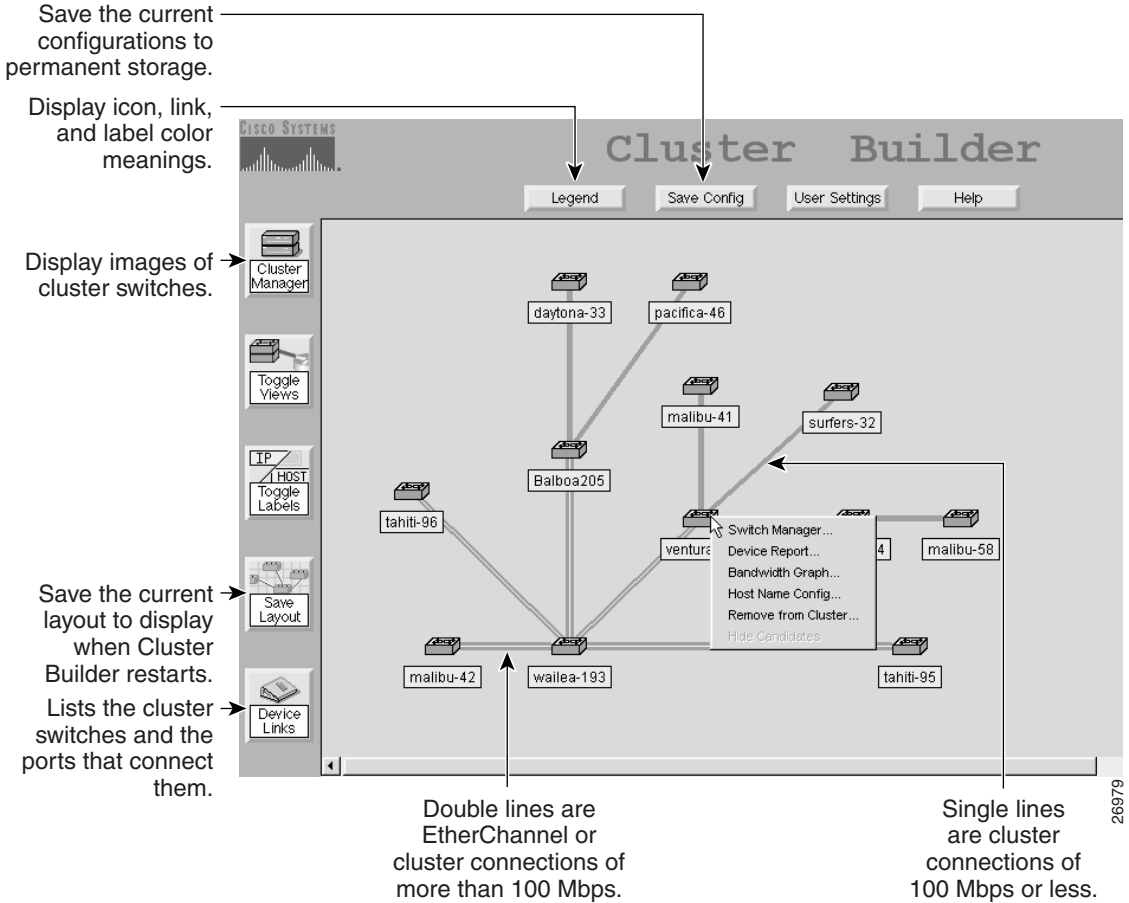
Adding and Removing Member Switches

You can use the network map in Cluster Builder to add switches to the cluster (Figure 4-2). Switches in the cluster have green labels, and candidates have blue labels. Right-click a candidate, and click **Add to Cluster** from the pop-up menu. If the candidate is in a different management VLAN than the command switch, a message is displayed indicating that this candidate is unreachable, and you will not be able to add it to the cluster.

You can add the candidate to the cluster if the maximum number of switches supported in the cluster has not been exceeded; otherwise, you must remove a member before adding a new one. If a password has been configured on the switch, you are prompted to enter it along with your username.

You can remove a member switch by right-clicking it and selecting **Remove from Cluster** from the pop-up menu. You can also use the CLI to remove a member switch. See the next section.

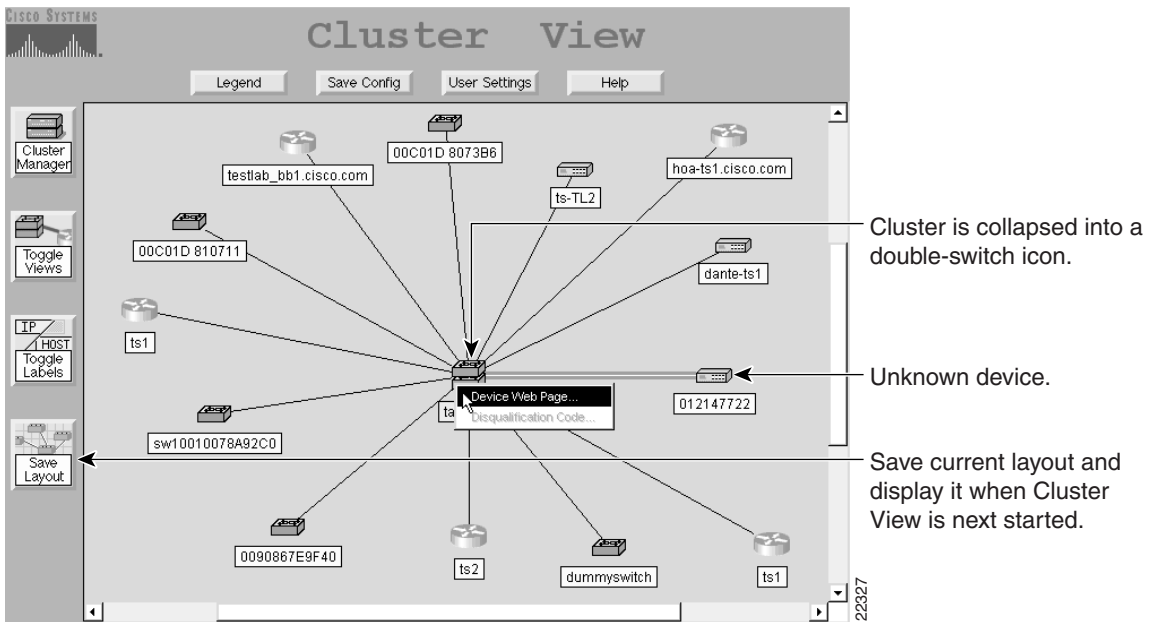
Figure 4-2 Cluster Builder



Determining Why a Switch is Not Added to the Cluster

If a switch does not become part of the cluster, display Cluster View by clicking the **Toggle Views** button in Cluster Builder. Cluster View displays the cluster as a double-switch icon and shows connections to devices outside of the cluster (Figure 4-3). Right-click the device (yellow label), and select **Disqualification Code** to display the reason it did not join the cluster.

Figure 4-3 Cluster View



CLI Procedure for Removing Member Switches

Beginning in privileged EXEC mode on the command switch, follow these steps to remove a member switch from the cluster:

Task	Command
Step 1 Display the status of the cluster, and note the MAC address and switch number of the switch you want to remove.	show cluster members
Step 2 Enter global configuration mode.	configure terminal
Step 3 Remove the switch from the cluster.	no cluster member <i>n</i>
Step 4 Return to privileged EXEC mode.	end
Step 5 Display the status of the new cluster.	show cluster members

You can remove a member switch from a cluster using the member switch CLI, but you must also enter commands on the command switch.

Beginning in privileged EXEC mode on a 2900 or 3500 XL member switch, follow these steps to remove it from a cluster:

Task	Command
Step 1 On the member switch, enter global configuration mode.	configure terminal
Step 2 Remove the member switch from the cluster.	no cluster commander-address
Step 3 Return to privilege EXEC mode.	end
Step 4 Verify that the member switch is no longer part of the cluster.	show cluster
Step 5 On the command switch, display the status of the cluster, and note the MAC address and switch number of the switch you want to remove.	show cluster members
Step 6 Enter global configuration mode.	configure terminal
Step 7 Remove the switch from the cluster.	no cluster member <i>n</i>

Task	Command
Step 8 Return to privileged EXEC mode	end
Step 9 Display the status of the new cluster.	show cluster members

For information on how to remove Catalyst 1900 or 2820 member switches, refer to the *Catalyst 1900 Series Installation and Configuration Guide* or the *Catalyst 2820 Series Installation and Configuration Guide*.

Arranging and Saving the Device Layout

You can reposition devices in Cluster Builder and Cluster View, and save this information for subsequent relaunching of the application. Before arranging and saving the layout, make sure the command switch discovers all devices or that you manually add them to the cluster that you want to manage.

You arrange the layout by clicking and holding the left mouse button on a device and dragging it to a new location on the map. You cannot move the command switch in Cluster Builder or the cluster icon in Cluster View. Click **Save Layout** to save the layout on the command switch.

When you relaunch Cluster Builder or Cluster View, it displays the saved version of the layout if the topology did not change. If a topology change occurs, you must arrange the devices again and click **Save Layout**.

If your switches are connected in a daisy-chain configuration, Cluster Builder discovers only devices that are one hop from the command switch. You must add devices one at a time to discover all of the devices in the daisy chain. After you have added all the devices in the daisy chain and arranged them to your liking, click **Save Layout**.

Changing User Settings

Click **User Settings** at the top of the Cluster View, Cluster Builder, or Cluster Manager page to change the parameters described in the following list. The user settings are automatically saved in permanent storage on the command switch.

- **Cluster Builder and Cluster Manager polling interval**—Select the number of seconds the switch waits before polling the switch for new cluster and port information. Lowering the polling interval can be useful when you are changing or testing the cluster switches. The default is 120 seconds.

When you change this parameter, you must reload the page in Netscape or refresh it in Internet Explorer for the new setting to take effect.

- **Link and device graph polling interval**—Select the number of seconds the switch waits before the application polls it for new graph information. The default is 24 seconds.

When you change this parameter, you must reload the page in Netscape or refresh it in Internet Explorer for the new setting to take effect.

- **Show suggested candidate window every time Cluster Management starts**—Set the switch to prompt the user with new candidates every time Cluster Builder or Cluster Manager is started. Cluster Builder still redraws the map of the network if new devices are discovered.

If you set the switch to always discover new candidates and you also have Cluster Manager set to display by default, you are prompted to display Cluster Builder to add or remove devices from the cluster.

- **Change the default view**—Select Cluster Manager to display by default when Cluster Management starts.

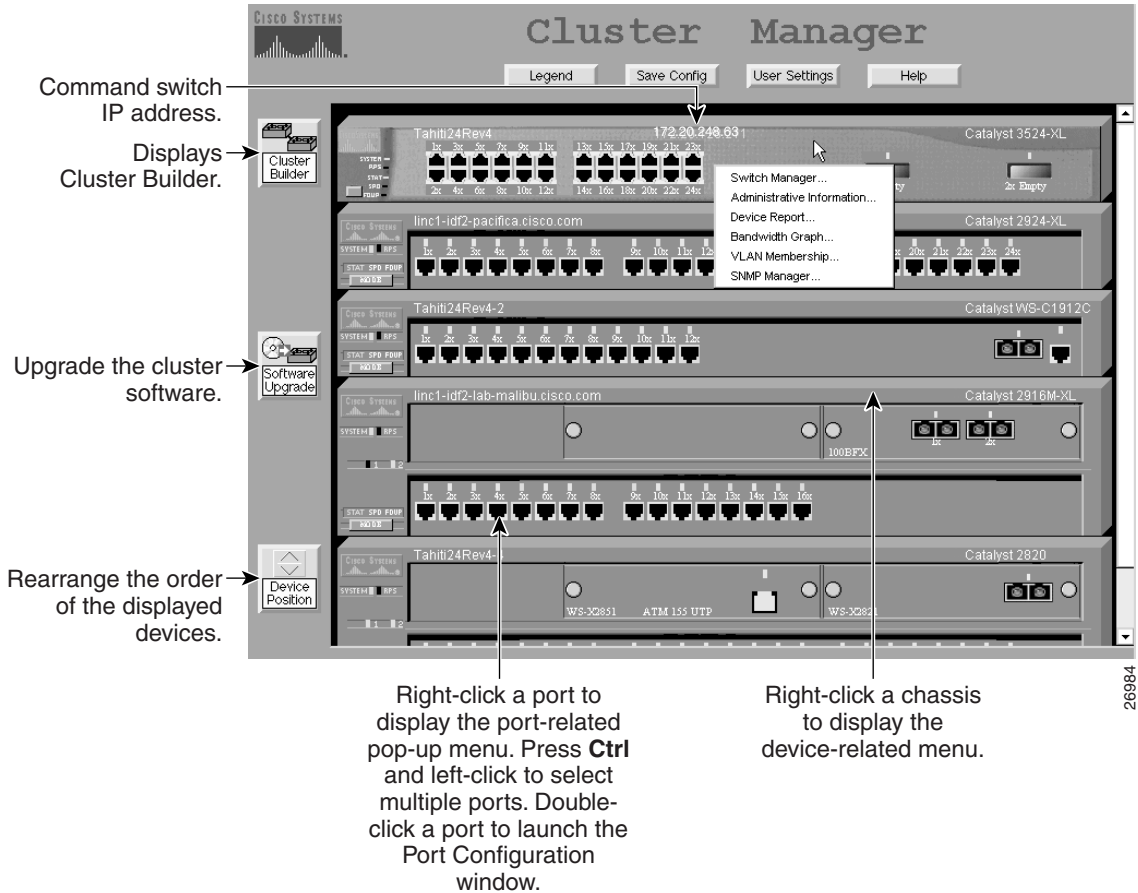
Managing Clusters

After you have created a cluster, you predominantly use Cluster Manager to monitor and configure the switches in the cluster. Figure 4-4 shows a cluster displayed in Cluster Manager. The switch software updates the LEDs displayed on these images in real time, making the images displayed by Cluster Manager as informative as the switch LEDs themselves. You can also use Cluster Builder and Cluster View to manage your cluster.

This section describes how to perform the following tasks:

- Save configuration changes
- Monitor and configure ports
- Display port connection information
- Change the host name
- Display VLAN membership information
- Upgrade the switch software on all switches in the cluster
- Enable and configure SNMP
- Rearrange the physical images of the switches
- Display performance graphs
- Display device reports
- Access single device web-management applications

Figure 4-4 Cluster Manager



Saving Configuration Changes

Configuration changes on the 2900 and 3500 XL switches are not written to Flash memory until you click the **Save Config** button that appears in Cluster Manager, Cluster Builder, and Cluster View. This button does not apply to Catalyst 1900 and 2820 switches, which automatically save configuration changes to Flash memory as they occur.

As you make cluster configuration changes (except for changes to the device layout and in the User Settings window), make sure you periodically click **Save Config** in any view. The configuration is saved on the command and member switches.

Monitoring Port Status

The LEDs above the ports (or the port openings) in Figure 4-4 can display the port status (STAT), speed (SPD), or duplex (FDUP) settings on 2900 and 3500 XL switches. The LEDs above the ports on Catalyst 1900 and 2820 switches display the status (STAT) and duplex (FDUP) settings. The STAT LED displays the link status of the port, SPD displays the speed of the port, and FDUP displays whether the port is operating in half- or full-duplex mode.

Note The UTIL LED on Catalyst 1900, 2820, 2900 XL, and 3500 XL switches is not displayed in Cluster Manager.

For more information about the switch LEDs, refer to the switch installation guide.

Click the **Mode** button on the image to highlight in turn each of the settings. Click **Legend** to display the meanings of the colors.

Changing the Polling Interval for Status Monitoring

Cluster Manager periodically polls the command switch for the status of all ports in the cluster to update the switch port status and to check for new members. You can change the polling interval by clicking the **User Settings** button and selecting a new interval from the Cluster Builder and Cluster Manager Polling Interval drop-down list. The default is 120 seconds.

A long polling interval reduces the load (number of requests) on the command switch, and topology updates are not reported as frequently. A short polling interval has the opposite affect. Cisco recommends that you use a short interval only for troubleshooting or while building a cluster.

When you change this parameter, you must reload the page in Netscape or refresh it in Internet Explorer for the new setting to take effect.

Configuring Ports

You can configure a single or multiple ports on the same switch by clicking them in Cluster Manager. For port-configuration guidelines, see the “Configuring Port Parameters” section on page 3-22. You can also display the settings for each port.

When you select a port or ports, you can set the following parameters:

Status: Administratively enables or disables the port.

Duplex: Catalyst 2900 and 3500 XL switches: sets a port to full-duplex (**Full**), half-duplex (**Half**), or autonegotiate (**Auto**). The default is **Auto**. For ATM ports, this field is read-only and displays **Full**.

Catalyst 1900 and 2820 switches: sets an Ethernet port to full-duplex (**Full**) or half-duplex (**Half**). The default is **Half**.

- On Fast Ethernet (100BaseTX) ports, sets the port to **Full**, **Half**, autonegotiate (**Auto**), or full duplex with flow control (**Full-Flow-Control**). The default is **Half**. However, the 100BaseTX module ports for the Catalyst 2820 switch do not autonegotiate.
- On Fast Ethernet (100BaseFX) ports, sets the port to **Full**, or **Half**, or **Full-Flow-Control**. The default is **Half**.
- For ATM and FDDI ports, this field is read-only and displays **Full**.

Speed: Sets a 10/100 port to 10 Mbps (**10**), 100 Mbps (**100**), or autonegotiate (**Auto**). The default is **Auto**.

You cannot configure this field on Catalyst 1900 and 2820 switches.

For Gigabit Ethernet ports, the field displays **1000** (1000 Mbps) and is read-only. For ATM ports, the field displays **155** (155 Mbps) and is read-only.

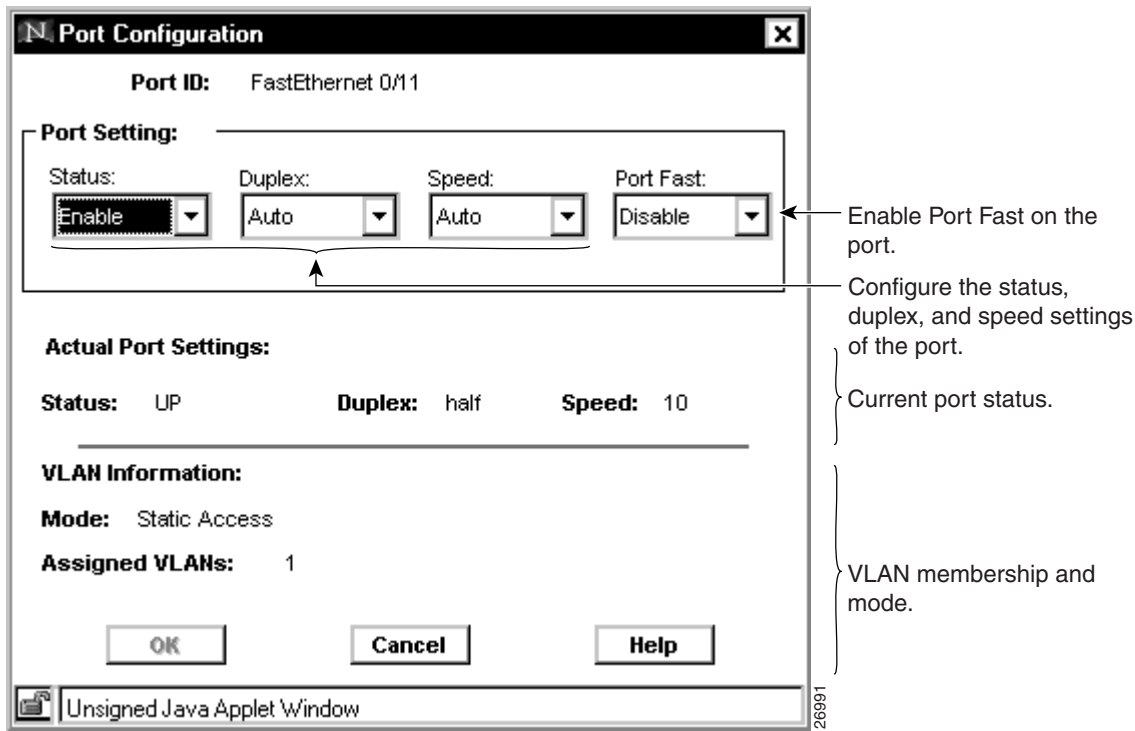
Port Fast: Sets the port to immediately enter the STP forwarding state and bypass the normal transition from the listening and learning states to the forwarding state.

Note The autonegotiation feature can sometimes cause unpredictable results. For more information on 2900 and 3500 XL autonegotiation mismatches, see the “Connecting to Devices That Do Not Autonegotiate” section on page 3-22.

Configuring a Single Port

To configure a single port, right-click it and then select **Port Configuration** (Figure 4-5) from the pop-up menu. You can also double-click a port to launch the Port Configuration window from which you can enable or disable the port, change the speed and duplex settings, and enable or disable the STP Port Fast parameter.

Figure 4-5 Single Port Configuration



Displaying Settings for a Single Port

When you configure a single port, the Port Configuration window displays the current status and the current settings of the port. In addition, the window displays the VLAN mode of the port and the VLANs that the port belongs to. For static-access VLAN ports, the VLAN ID is displayed. For trunk ports, the trunk type (ISL, 802.1Q, or ATM) is displayed in the Mode field. For multi-VLAN ports, a string of VLAN IDs is displayed in the Assigned VLANs field.

If your Catalyst 1900 or 2820 switch is running standard edition software or running Enterprise Edition Software with bridge groups enabled, the VLAN Information section is not displayed.

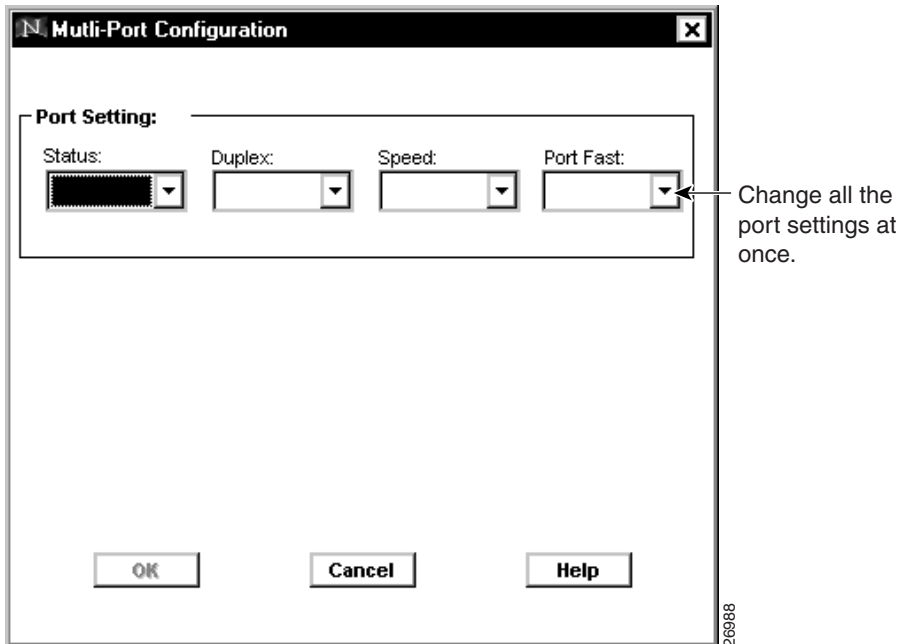
Configuring Multiple Ports

To configure multiple ports on the same switch, left-click them while holding down the **Ctrl** key. After selecting the ports, right-click to display the pop-up menu, and select **Port Configuration**. The Multi-Port Configuration window (Figure 4-6) displays. You can use this window to change the ports settings for the selected ports, but the window does not display the actual port settings or VLAN information.

While you can configure settings for multiple mixed ports, some settings may not apply to all ports. For example, you can select half duplex from the drop-down list for a mixture of Ethernet, Gigabit Ethernet, and ATM ports, but the application applies the setting only to Ethernet and Gigabit Ethernet ports.

For more information on configuring 2900 and 3500 XL ports, see the “Configuring Port Parameters” section on page 3-22 or click **Help**.

Figure 4-6 Multi-Port Configuration



Displaying Port Connection Information

You can see how the cluster members are interconnected by using the Cluster Builder network map. It shows how the switches are connected and the type of connection between each device. Click **Legend** in Cluster Builder to learn the meaning of each icon, link, and color.

You can display port connection information in two ways: **Toggle Labels** and **Device Links** buttons. By clicking **Toggle Labels**, you can see the port numbers for each end of the link. By clicking **Device Links**, you can see a connection report for all devices in the cluster.

Changing the Host Name

You can change the host name of any switch in the cluster by using Cluster Manager or Cluster Builder.

To change the host name on a member switch in Cluster Manager, right-click the chassis and select **Administrative Information** from the pop-up menu. In the Administrative Information window, you can change the host name, system contact, and system location information.

To change the host name on a member switch in Cluster Builder, right-click the switch, and select **Host Name Config** from the pop-up menu. Enter a unique host name into the field, and click **OK**.

Member switch host names must be unique in the cluster and no longer than 31 characters. Do not use a “-N” (where n is a number) as the last characters in a host name on any switch.

When you change the host name on the command switch, assign a name no longer than 28 characters. Limiting the command switch host name to 28 characters ensures that each member switch host name is unique and viewable in the application. Recall that the command switch appends a member number to its host name and propagates it to new switches not originally configured with a name when they join the cluster.

Displaying VLAN Membership

The VLAN Membership window (Figure 4-7) displays the list of all the user-defined VLANs on the switch. By selecting a VLAN, you can display the ports that belong to the VLAN. In addition, the color coding indicates which VLAN mode a port is in.

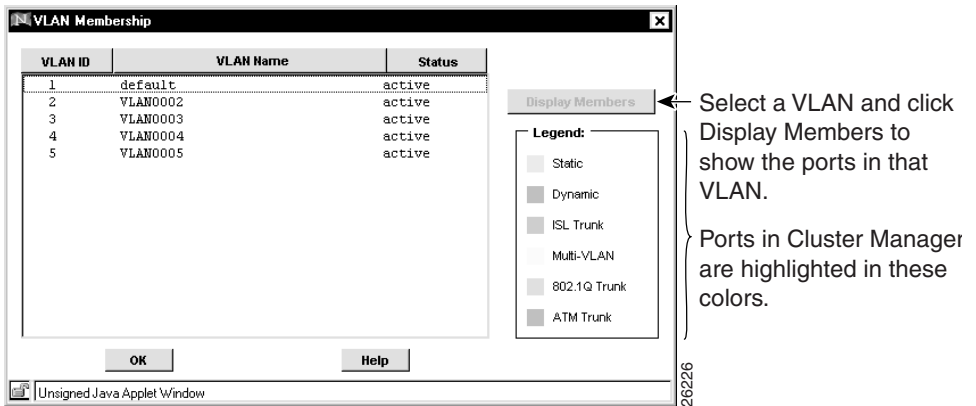
To display the VLANs that are active on a switch, right-click the chassis of the switch in Cluster Manager, and select **VLAN Membership** from the pop-up menu.

If your Catalyst 1900 or 2820 switch is running standard edition software or running Enterprise Edition Software with bridge groups enabled, the **VLAN Membership** menu item is not available (grayed out).

To display the ports that belong to a given VLAN, select the VLAN ID on the VLAN Membership window, and click **Display Members**. Cluster Manager highlights on the switches all the ports that belong to the selected VLAN. You may need to move the VLAN Membership window to see the ports highlighted in Cluster Manager. The Legend on the VLAN Management window indicates the VLAN type (static, dynamic, trunk, and so forth).

You can also display VLAN membership information on the Port Configuration window in Cluster Builder. For more information, see “Displaying Settings for a Single Port” section on page 4-23.

Figure 4-7 VLAN Membership



Upgrading Software for a Group of Switches

You can upgrade cluster switches by using the Software Upgrade window (Figure 4-8) in Cluster Manager. New software releases are posted on Cisco Connection Online (CCO) and are available through authorized resellers. You can also download the Cisco TFTP server from CCO.

You can upgrade all or some of the switches in a cluster at once, but the software performs a series of checks before the upgrade takes place. To speed the upgrade process, follow these rules:

- Do not upgrade switches from different product lines at the same time. Separate 2900 from 3500 XL switches. However, you can group together and upgrade Catalyst 1900 and 2820 switches.
- Do not upgrade 2900 XL switches with 4 MB of DRAM to an 8-MB image. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. These switches must run IOS Release 11.2(8.x)SA6 original edition software to be cluster members. No original edition software package is available for the IOS Release 12.0(5)XP. To determine the switch DRAM size, enter the user-level **show version** command.
- Do not install the original edition software for switches with 4 MB of DRAM onto 2900 and 3500 XL switches with 8 MB of DRAM.
- Upgrade Catalyst 1900 and 2820 switches last. These switches need to be rebooted shortly after the upgrade occurs to function efficiently. If you do not click the **Reboot Cluster** button in 30 seconds after the upgrade, the Catalyst 1900 and 2820 switches automatically reboot.
- For 2900 and 3500 XL switches, enter the *image_name.tar* filename into the New File Name field. The tar file contains both the IOS image and the web management code.
- For Catalyst 1900 and 2820 switches, enter the *image_name.bin* filename into the New File Name field. The bin file contains the software image and the web management code.

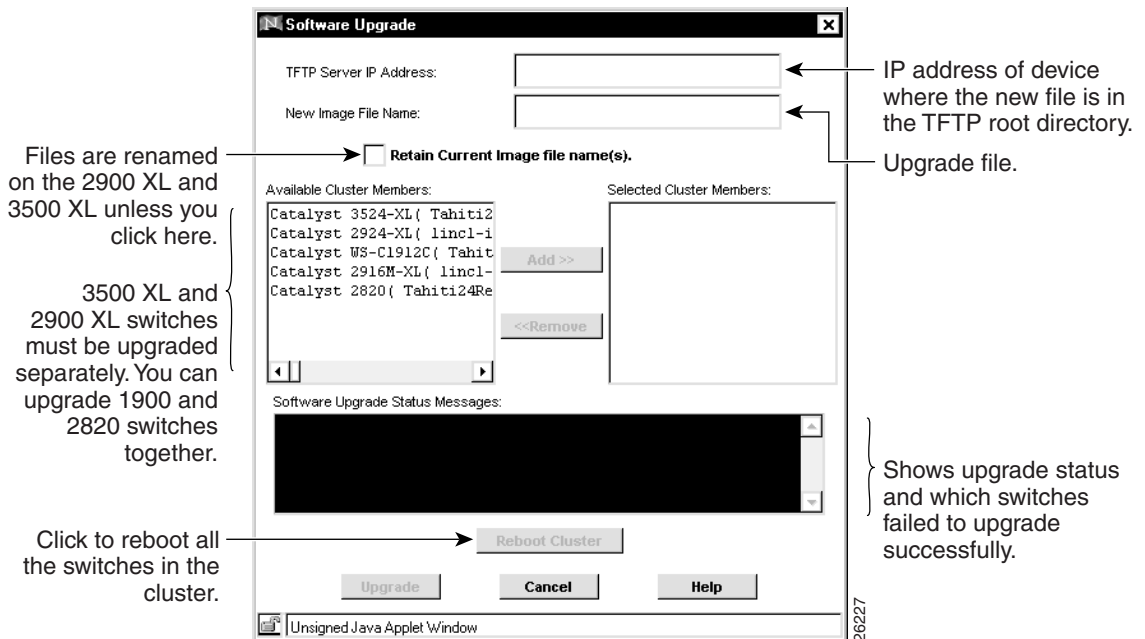
When you use the software upgrade page, enter a tar filename (for 2900 and 3500 XL switches) or a bin filename (for Catalyst 1900 and 2820 switches) that contains the switch software image and the web management code. You can enter just the filename or a path into the New Image File Name field. You do not need to enter a path if the image file is in the TFTP server root directory.

On 2900 and 3500 XL switches, new images are copied to Flash memory and do not affect the operation of the switch. The switch checks Flash memory to ensure there is sufficient space before the upgrade takes place. If there is not enough space in Flash memory for the new and old image, the new image replaces the old one during the upgrade. If there is enough space, the new image is copied to the switch without replacing the old image. Only after the new image is completely downloaded is the old one erased. If you experience a failure during the copy process, you can still reboot your switch using the old image.

On Catalyst 1900 and 2820 switches, the new image overwrites the current image during the upgrade.

New features provided by the software are not available until you reload the software.

Figure 4-8 Cluster Software Upgrade



Configuring the Cisco TFTP Server to Upgrade Multiple Switches

The Cisco TFTP server application can handle multiple requests and sessions, but you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

CLI Procedure for Upgrading Catalyst 2900 or 3500 XL Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch. Follow these steps to upgrade the software on a 2900 or 3500 XL member switch:

Step 1 In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, get the number of the member switch that needs to be upgraded. The member number is listed in the SN column of the display. You need the member number for Step 2.

Step 2 Log into the member switch (for example, member number 1):

```
switch# rcommand 1
```

Step 3 Start the TFTP copy as if you were initiating it from the command switch.

```
switch-1# tar /x tftp://server_ip_address//path/filename.tar  
flash:  
Source IP address or hostname [server_ip_address]?  
Source filename [path/filename]?  
Destination filename [flash:new_image]?  
Loading /path/filename.bin from server_ip_address (via!)  
[OK - 843975 bytes]
```

Step 4 Reload the new software with the following command:

```
switch-1# reload  
System configuration has been modified. Save? [yes/no]:y  
Proceed with reload? [confirm]
```

You lose contact with the switch while it reloads the software. For more information on the **rcommand**, see the “Understanding the CLI” section on page 2-30.

CLI Procedure for Upgrading Catalyst 1900 or 2820 Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch. Follow these steps to upgrade the software on a Catalyst 1900 or 2820 member switch:

- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, get the number of the member switch that needs to be upgraded. The member number is listed in the SN column of the display. You need the member number for Step 2.

- Step 2** Log into the member switch (for example, member number 1):

```
switch# rcommand 1
```

- Step 3** For switches running standard edition software, enter the password (if prompted), access the Firmware Configuration menu from the menu console, and perform the upgrade.

The Telnet session accesses the menu console (the menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 1, you are prompted for the password before accessing the menu console.

Follow the instructions in the installation and configuration guide that shipped with your switch. When the download is complete, the switch resets and begins using the new software.

- Step 4** For switches running Enterprise Edition Software, start the TFTP copy as if you were initiating it from the member switch.

```
switch-1# copy tftp://host/src_file opcode
```

For example, **copy tftp://spaniel/op.bin opcode** downloads new system operational code *op.bin* from host *spaniel*.

You should see the TFTP successfully downloaded operational code message. When the download is complete, the switch resets and begins using the new software.

You can also perform the upgrade through the menu console Firmware Configuration menu. For more information, refer to the switch installation and configuration guide.

You lose contact with the switch while it reloads the software. For more information on the **recommand**, see the “Understanding the CLI” section on page 2-30.

Configuring SNMP

The command switch manages SNMP communication for all switches in the cluster. The command switch forwards the set and get requests from SNMP applications to member switches, and it forwards the traps and other responses coming from the member switches to the appropriate management station.

Enabling or Disabling the SNMP Agent

You can enable or disable the SNMP agent on your cluster switches. By default, the SNMP agent is enabled on the Catalyst 2900 XL, 3500 XL, 1900, and 2820 switches. You cannot disable the agent on Catalyst 1900 and 2820 switches.

SNMP must be enabled for the Cluster Management features to work properly.

Configuring Community Strings

Use the SNMP Manager window (Figure 4-9 and Figure 4-10) to enter read-write and read-only community strings on individual cluster switches. Community strings provide authentication in the exchange of SNMP messages.

The Catalyst 2900 and 3500 XL switches support an unlimited number of community strings of any length. When you configure a community string for these switches using SNMP Manager, do not use the @esN notation (N is the member switch number) because this information is automatically appended to each string.

When a 2900 or 3500 XL member switch is removed from the cluster, community strings ending in @esN are removed. If the switch rejoins a cluster at a later time, the first read-only and read/write community strings from the command switch are appended with an @esN and propagated to the member switch.

The Catalyst 1900 and 2820 switches support up to four read-only and four read/write community strings that are 32 characters in length. Because a read-only and read/write community string from the command switch was propagated to the switch when it joined the cluster, you can configure up to three additional read-only and three read/write community strings. When you configure community strings for these switches through the SNMP Manager window, limit the string length to 27 characters because the @esN, where N can be up to two digits, is automatically appended to each string. Do not use the @esN notation in any community string you configure. If you enter a string longer than 27 characters, it is truncated to 27.

When a Catalyst 1900 or 2820 member switch is removed from the cluster, community strings ending in @esN are removed. If the switch rejoins a cluster at a later time, the first read-only and read/write community strings from the command switch are appended with an @esN and propagated to the member switch.

Note When removing community strings from cluster members, make sure **not** to remove the community strings propagated from the command switch when the switch joined the cluster. If you remove the propagated community string, the command switch cannot route SNMP packets to the member switch. On 2900 and 3500 XL switches, the first read-only and read-write community string listed in the SNMP Manager window is propagated from the command switch. On Catalyst 1900 and 2820 switches, the last read-only and last read-write community string listed in the SNMP Manager window is propagated from the command switch.

Figure 4-9 SNMP Manager for Catalyst 2900 and 3500 XL Switches

Click one to allow or disallow SNMP applications access to the switch.

Enter a character string to authenticate SNMP requests.

Click to display MIB object information.

Click to display and set MIB objects.

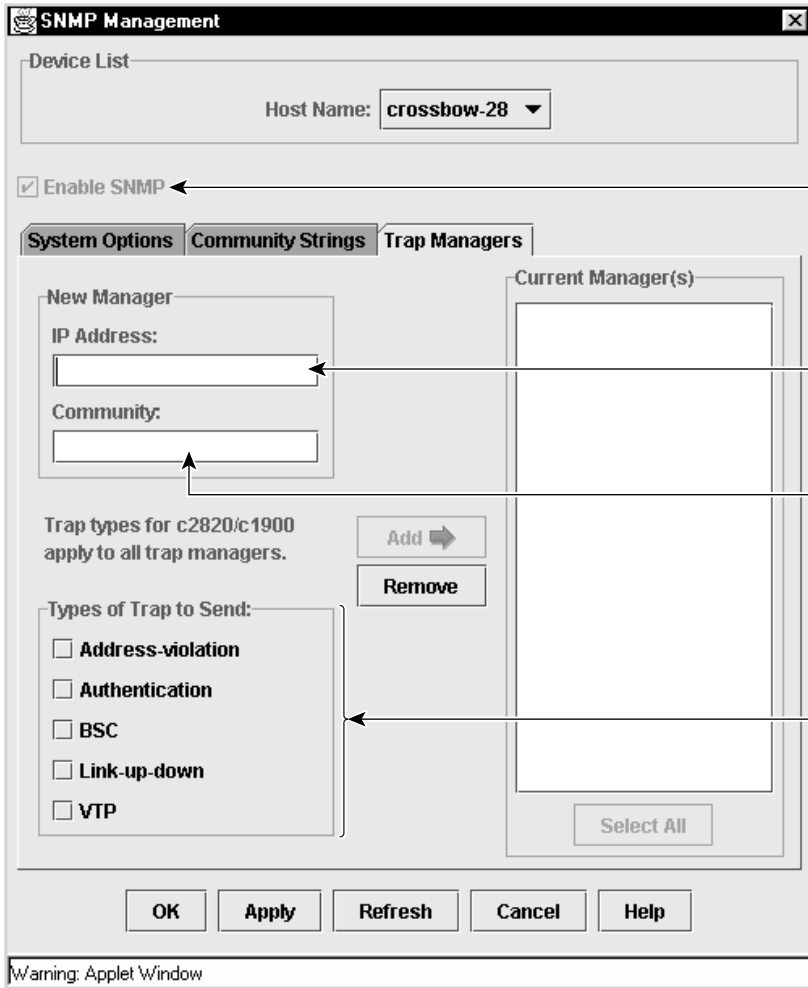
Enter the IP address of PC or workstation to receive traps.

Enter a character string to act as a password for the trap manager.

Unsigned Java Applet Window

26995

Figure 4-10 SNMP Manager for Catalyst 1900 and 2820 Switches



You cannot disable the SNMP agent on Catalyst 1900 and 2820 switches.

Enter the IP address of PC or workstation to receive traps.

Enter a character string to act as a password for the trap manager.

Catalyst 1900 and 2820 traps.

Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. The command and member switches have individual trap managers and trap types configured directly on them. When a member switch issues a trap, it is sent to the trap manager by using the member switch IP address. If the member switch does not have an IP address, the trap is sent through the command switch.

The command switch does not propagate its trap manager addresses or trap community strings to cluster members. By default, no trap manager is defined, and no traps are issued.

The 2900 and 3500 XL switches support an unlimited number of trap managers. Community strings can be any length. When you configure a community string for these switches, do not use the @esN notation because this information is automatically appended to each string.

Table 4-1 describes the 2900 and 3500 XL switch traps. You can enable any or all of these traps and configure them to be received by a specific trap manager.

Table 4-1 Catalyst 2900 and 3500 XL Switch Traps

Trap Type	Description
Config	Generates a trap when the switch configuration changes.
TTY	Generates a trap when the switch starts a management console CLI session.
VTP	Generates a trap for each VLAN Trunk Protocol (VTP) changes (Enterprise Edition Software only).
SNMP	Generates the supported SNMP traps.
VLAN Membership	Generates a trap for each VLAN Membership Policy Server (VMPS) change (Enterprise Edition Software only).
C2900/C3500	Generates the switch-specific traps. These traps are in the private enterprise-specific MIB

Catalyst 1900 and 2820 switches support up to four trap managers. When you configure community strings for these switches through SNMP Manager, limit the string length to 32 characters. When configuring traps on Catalyst 1900 and 2820 switches, you cannot configure individual trap managers to receive specific traps.

Table 4-2 describes the Catalyst 1900 and 2820 switch traps. You can enable any or all of these traps, but these traps are received by all configured trap managers.

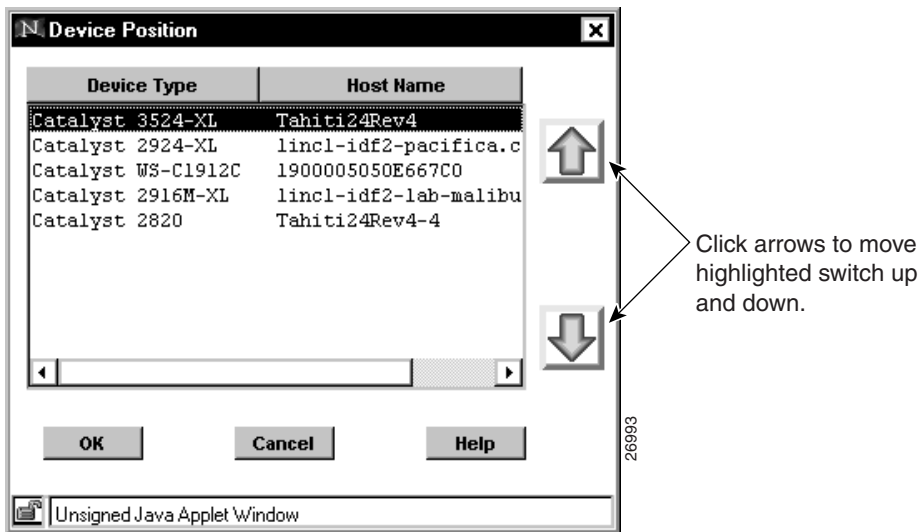
Table 4-2 Catalyst 1900 and 2820 Switch Traps

Trap Type	Description
Address-violation	Generates a trap when the address violation threshold is exceeded.
Authentication	Generates a trap when an SNMP request is not accompanied by a valid community string.
BSC	Generates a trap when the broadcast threshold is exceeded.
Link-up-down	Generates a link-down trap when a port is suspended or disabled for any of these reasons: <ul style="list-style-type: none">• Secure address violation (address mismatch or duplication)• Network connection error (loss of linkbeat or jabber error) User disabling the port Generates a link-up trap when a port is enabled for any of these reasons: <ul style="list-style-type: none">• Presence of linkbeat• Management intervention• Recovery from an address violation or any other error• STP action
VTP	Generates a trap when VTP changes occur (Enterprise Edition Software only).

Rearranging the Order of the Switches

You can arrange the order in which switches are displayed in Cluster Manager to match the arrangement in your wiring closet. Click the Device Position button to display the Device Position window (Figure 4-11). Select a device in the Device Position window, and use the arrows to move it up or down in the list. Click **OK** when you are finished.

Figure 4-11 Device Position



Displaying Link Utilization Graphs

You can use Cluster Builder, Cluster Manager, and Cluster View to display real-time graphs that can help you analyze traffic patterns and identify problems with individual links. To display a link graph, one end of the link must be connected to a port on a cluster member that is a 2900 or 3500 XL switch. Links between Catalyst 1900 and 2820 switches, Catalyst 2820 and 2820 switches, or Catalyst 1900 and 1900 switches cannot be graphed. Before you can generate graphs, you must enable SNMP and set the community string to *public*.

Displaying Link Utilization Graphs

To display a link graph in Cluster Builder or Cluster View, right-click a link and select **Link Graph** from the pop-up menu. To display a link graph in Cluster Manager, right-click a port that has a green status LED, and select **Link Graph** from the pop-up menu.

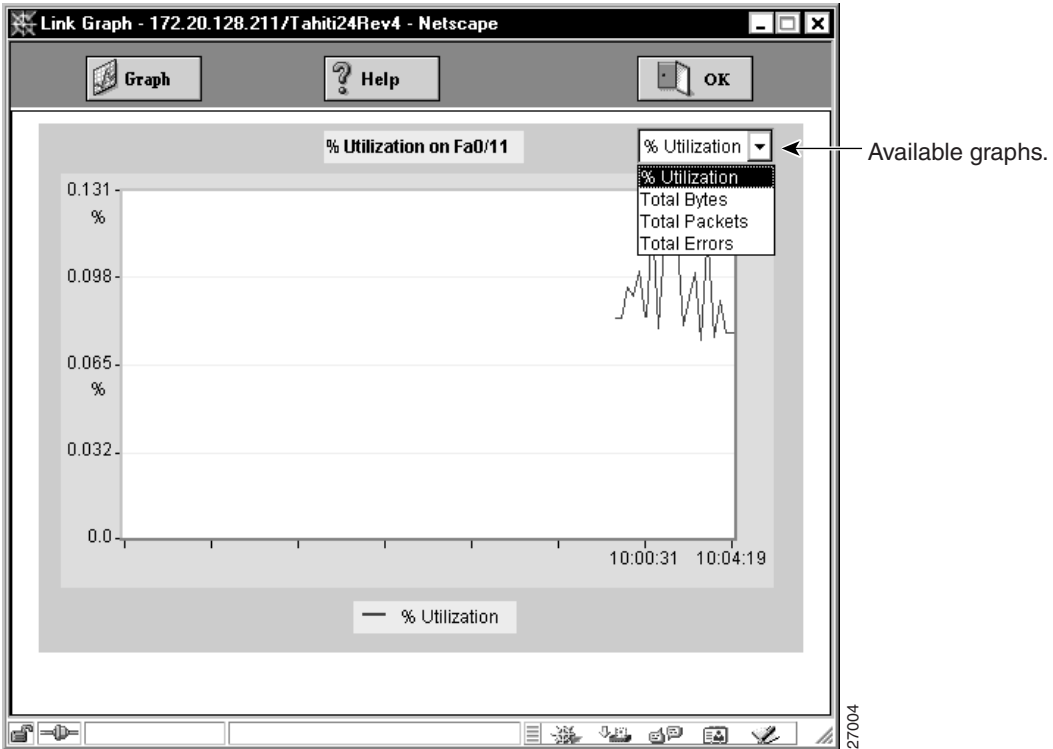
The graph runs as a separate browser session and can run in the background without interrupting the original session. The host name of the switch is displayed in the browser window title bar, and the link port number is displayed above the graph.

When the graph window is displayed (Figure 4-12), use the drop-down list in the upper right corner to select the data you want to present.

Select one of the following graphs from the drop-down list:

- Percent utilization (Figure 4-12)
- Total number of bytes sent and received (Figure 4-13)
- Packets sent and received, including broadcast and multicast packets
- Total errors, including error packets and dropped packets

Figure 4-12 Link Graph (Percent Utilization)



Displaying the Percent Utilization

This graph (Figure 4-12) displays the percentage of the maximum bandwidth in use by the port number displayed on the graph.

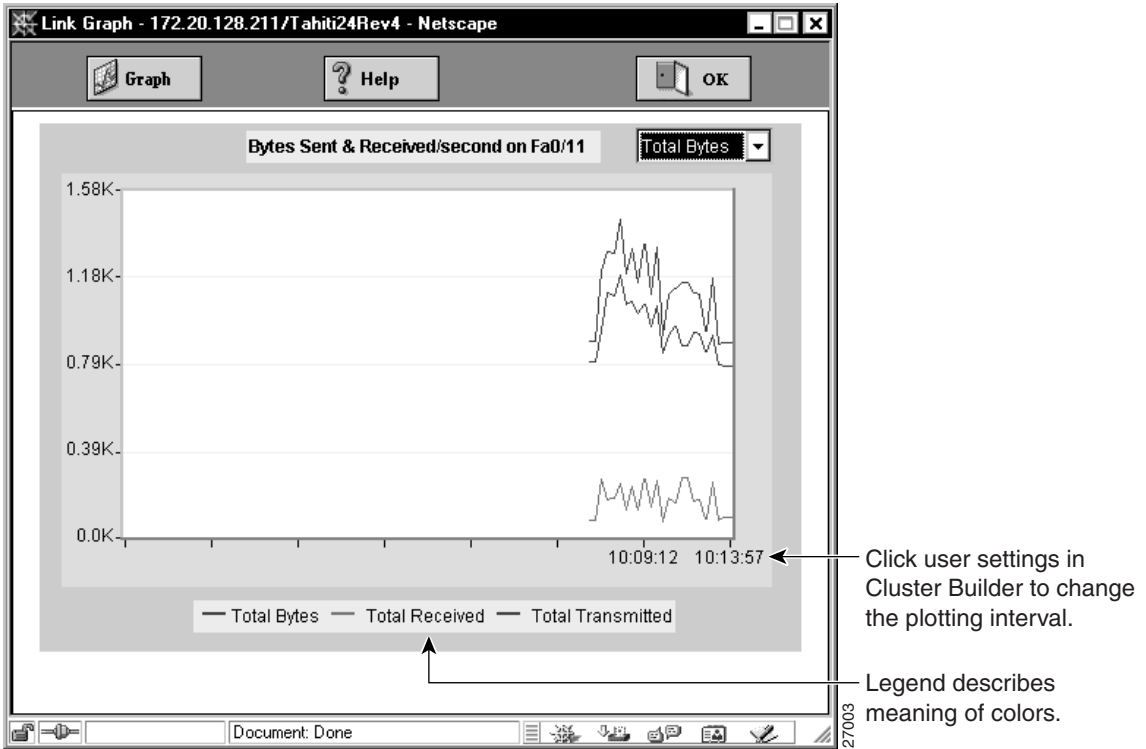
Displaying Total Bytes Sent and Received on a Link

This graph (Figure 4-13) displays the number of bytes sent and received by the port number displayed on the graph.

The following colors represent three different graphs:

- Blue—Total number of bytes sent and received on the port
- Red—Total number of bytes received on the port
- Black—Total number of bytes sent on the port

Figure 4-13 Total Bytes Sent and Received



Displaying Total Number of Packets Sent on a Link

This graph displays the number of packets sent and received by the port number displayed on the graph. The following colors represent the two graphs:

- Blue—Total number of packets sent and received on the port
- Red—Total number of broadcast and multicast packets sent and received on the port

Displaying the Total Errors on a Link

This graph displays the total number of errors sent and received by the port number displayed on the graph. The following colors represent the two graphs:

- Blue—Total number of packets with errors sent and received on the port
- Red—Total number of packets dropped by the port

Displaying Device Reports and Graphs

Cluster Management can extract real-time information from 2900 and 3500 XL member switches and present it in the form of device reports and graphs. Device reports and graphs are not available for Catalyst 1900 and 2820 switches. Before you can generate reports and graphs, you must enable SNMP and set the community string to *public*.

You can display the device report by using Cluster Builder and Cluster Manager. In Cluster Builder, right-click a cluster member and select **Device Report** from the pop-up menu. In Cluster Manager, right-click a chassis and select **Device Report** from the pop-up menu.

Each device report displays with a drop-down list in the upper right corner. From the drop-down list, you can display the following reports:

- Config Information (Figure 4-14)
- System Information (Figure 4-15)
- Port Information (Figure 4-16)

From any of the device report pages, you can generate a graph of the switch bandwidth by clicking **Graph**. The graph provides an estimate of the traffic flowing through the switch. You can display this same graph from Cluster Builder by selecting **Bandwidth Graph** from the device pop-up menu.

From the Port Information Device Report page, you can generate a graph of the utilization percentage and the total packets, bytes, and errors recorded on the link corresponding to the port. To display this graph, select a green port button, and click **Graph**.

Figure 4-14 Config Information Device Report

The screenshot shows a software interface for displaying device reports. At the top, there is a navigation bar with buttons for 'Device Report', 'Graph', 'Switch Manager', 'Help', and 'OK'. An arrow points from the text 'Refresh the report.' to the 'Device Report' button. Below the navigation bar, the main content area displays information for a device named 'Tahiti-24'. The IP address is '172.20.128.27' and the configuration is 'Config Information'. A dropdown menu is shown next to the configuration name, with an arrow pointing to it from the text 'Display drop-down list of choices.'. The 'Description' field contains a text area with the following text: 'Cisco Internetwork Operating System Software', 'IOS (tm) C3500XL Software (C3500XL-C3H2B-M), Version', and 'Copyright (c) 1986-1999 by cisco Systems, Inc.'. An arrow points to this text area from the text 'IOS version running the switch.'. Below the description, there are fields for 'Location:' and 'Contact:'. The 'Member IP address:' is '172.20.128.27' and the 'Mask:' is '255.255.255.0'. The 'Default gateway:' is '172.20.128.1'. A bracket groups these IP-related fields with an arrow pointing to the text 'Switch IP Information.'. The 'Domain name:' field is empty. At the bottom, 'CDP:' is 'Enabled' and 'STP (VLAN1):' is 'Enabled'. A vertical number '26228' is visible in the bottom right corner of the interface.

Displaying Device Reports and Graphs

Figure 4-15 System Information Device Report

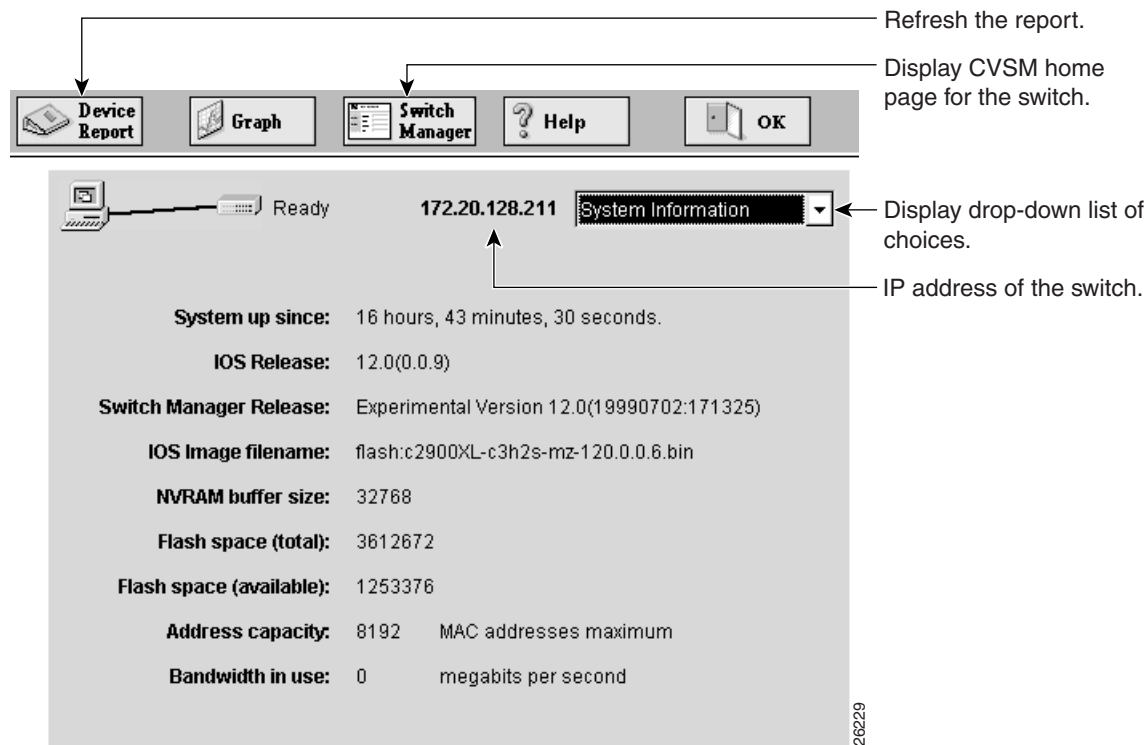


Figure 4-16 Port Information Device Report

The screenshot shows the CVSM interface for displaying a port information report. At the top, a navigation bar contains buttons for 'Device Report', 'Graph', 'Switch Manager', 'Help', and 'OK'. Below this, the main window displays the IP address '172.20.128.211' and a 'Port Information' dropdown menu. A 'Select a port:' section features a grid of 26 numbered ports, with port 11 selected. The selected port's details are shown below, including the MAC address '00:d0:79:64:1f:0c', the port name 'Fa0/11', and settings for 'Full duplex', 'Speed: 10 MB', and 'Admin status: Up'. A 'List learned addresses' button is present, with a list of two MAC addresses: '00:50:50:e6:67:c0' and '00:50:50:e6:67:cc'. Annotations with arrows point to various elements: 'Refresh the report.' points to the 'Device Report' button; 'Display CVSM home page for the switch.' points to the 'Switch Manager' button; 'Click to display drop-down list of choices.' points to the 'Port Information' dropdown; 'Port MAC address.' points to the MAC address field; 'Click to display addresses learned by the port.' points to the 'List learned addresses' button; and 'Addresses learned by the port.' points to the list of MAC addresses. A vertical number '26230' is located at the bottom right of the interface.

Performing Individual Device Configuration

You can access individual device configuration applications from Cluster View, Cluster Builder, and Cluster Manager.

In Cluster View, right-click a device and select **Device Web Page** from the pop-up menu. The management application for that device launches. For 2900 and 3500 XL switches, CVSM launches; for Catalyst 1900 and 2820 switches, switch manager launches. You can also double-click any device to launch its device configuration application.

In Cluster Builder, right-click a member switch and select **Switch Manager** from the pop-up menu. You can also right-click a candidate switch and select **Device Web Page** to launch its device configuration application. You can also double-click any device to launch its device configuration application.

In Cluster Manager, right-click a chassis and select **Switch Manager** from the device pop-up menu. You can also double-click a chassis and launch CVSM for 2900 and 3500 XL switches or launch switch manager for Catalyst 1900 and 2820 switches.